

Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols

Fei Gao, Su-Juan Qin, Fen-Zhuo Guo, and Qiao-Yan Wen

Abstract—Cryptanalysis is an important branch in the study of cryptography, including both the classical cryptography and the quantum one. In this paper we analyze the security of two three-party quantum key distribution protocols (QKDPs) proposed recently, and point out that they are susceptible to a simple and effective attack, i.e. the dense-coding attack. It is shown that the eavesdropper Eve can totally obtain the session key by sending entangled qubits as the fake signal to Alice and performing collective measurements after Alice's encoding. The attack process is just like a dense-coding communication between Eve and Alice, where a special measurement basis is employed. Furthermore, this attack does not introduce any errors to the transmitted information and consequently will not be discovered by Alice and Bob. The attack strategy is described in detail and a proof for its correctness is given. At last, the root of this insecurity and a possible way to improve these protocols are discussed.

Index Terms—Quantum cryptography, Quantum key distribution, quantum network communication, cryptanalysis, dense coding.

I. INTRODUCTION

CRYPTOGRAPHY IS the approach to protect data secrecy in public environment. As we know, the security of most classical cryptosystems is based on the assumption of computational complexity. But it was shown that this kind of security might be susceptible to the strong ability of quantum computation [1], [2]. That is, many existing cryptosystems will become no longer secure once quantum computer appears.

Fortunately, this difficulty can be overcome by quantum cryptography [3], [4]. Different from its classical counterpart, quantum cryptography is the combination of quantum mechanics and cryptography, where the security is assured by physical principles such as Heisenberg uncertainty principle and quantum no-cloning theorem. Now quantum cryptography has attracted a great deal of attentions because it can stand against the threat from an attacker with the ability of quantum computation. Quite a few branches of quantum cryptography have been studied in recent years, including quantum key distribution (QKD) [5], [6], [7], [8], [9], [10], quantum secret sharing (QSS) [11], [12], [13], quantum secure direct communication (QSDC) [14], [15], [16], [17], [18], quantum identity authentication [19], [20], [21], and so on.

As the most important application of quantum cryptography, QKD allows that two users, generally called Alice and Bob, can privately share a random key by using quantum carriers. The QKD protocols are designed carefully so that any effective eavesdropping will result in distortion of the quantum states

and then be discovered by the legal users. The fact that legal users can discover potential eavesdroppings is the key point of the security of QKD. If eavesdroppings are detected, the transmitted key, essentially a sequence of random bits, will be discarded. Otherwise, a secure key will be shared and it can be employed to encrypt the secrets communicated between Alice and Bob.

Obviously, quantum devices (QDs) are necessary to realize a QKD protocol, including the devices to generate qubits, to store qubits, to measure qubits, to perform unitary operations, and so on. For example, in the famous BB84 protocol [5], Alice has to generate qubits in four different quantum states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, while Bob needs to execute measurements in two different bases $B_z = \{|0\rangle, |1\rangle\}$ and $B_x = \{|+\rangle, |-\rangle\}$. Here $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. However, QDs are still expensive because qubits are quite difficult to deal with. In fact this is also the main reason why quantum cryptography has not been widely used in our daily life. Therefore, it is desirable to design protocols where some QDs are shared by different users. To this aim, a new QKD model, i.e. three-party QKD [22], [23], [24], appeared. Till now, most QKD protocols are two-party ones. That is, only two users, Alice and Bob, are concerned. In three-party QKD, another participant, i.e. the center, is introduced to help Alice and Bob to distribute the key. Furthermore, the center is equipped most of QDs while the users has less. When this kind of QKD is implemented in a network, one center can provide service to many users. By this means expensive QDs are shared and the expense of every user is reduced. As a result, three-party version is an effective manner to keep down the cost of QKD.

As we know, design and analysis has always been important branches of cryptography. Both of them drive the development of this field. In fact, cryptanalysis is an important and interesting work in quantum cryptography. As pointed out by Lo and Ko, *breaking cryptographic systems was as important as building them* [25]. In a QKD protocol, it is generally supposed that the quantum channel can be attacked with any manner allowed by quantum mechanics, while the classical one can only be listened but cannot be modified [3], [5]. In this situation, we say an attack strategy is successful if the eavesdropper Eve can elicit all or part of the secret key without being discovered by Alice and Bob.

Though in quantum cryptography legal users generally have the ability of discovering potential eavesdroppings, not all proposed protocols can achieve their expected security. Some protocols were attacked successfully by subtle strategies which were not concerned when these protocols were originally designed. Quite a few effective attack strategies have been proposed, such as intercept-resend attack [26], entanglement-

All authors are with State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: gaofei_bupt@hotmail.com; qsujuan@bupt.edu.cn; gfenzhuo@bupt.edu.cn; wqy@bupt.edu.cn).

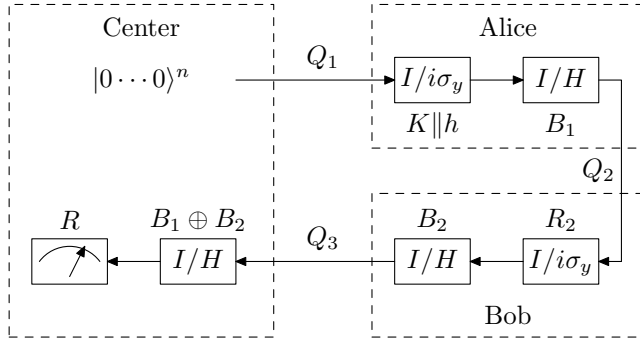


Fig. 1. The process of QKDP-I. For the sake of simplicity, all classical communications are omitted.

swapping attack [27], teleportation attack [28], [29], [30], channel-loss attack [31], [32], Denial-of-Service (DoS) attack [33], [34], Correlation-Extractability (CE) attack [35], [36], [37], Trojan horse attack [38], [39], participant attack [40], [41], [42], and so on. Understanding those attacks will be helpful for us to design new schemes with high security.

Recently Shih, Lee, and Hwang presented two novel three-party QKD protocols [24], where one is executed with an honest center and the other is with an untrusted center. Here “honest” means the center always follows the designed procedures to execute the protocol, and “untrusted” implies the center might cheat Alice and Bob, and try to elicit the key like an attacker. In this paper, we analyze the security of these two three-party QKD protocols and show that Eve can obtain the whole key transmitted between Alice and Bob without being detected by legal users. This attack is based on the technique of dense coding [43], which was also used in pervious strategies [41], [42].

The rest of this paper is organized as follows. The next section describes the three-party QKD protocols in Ref. [24] and introduces dense coding. In section III the particular attack strategy is demonstrated, and some useful discussions, including how to improve the protocols, are given in Section IV. Finally, a short conclusion is given in Section V.

II. PREVIOUS WORKS

In this section we will describe the three-party QKD protocols presented in Ref. [24] and a special feature of quantum entanglement, i.e. dense coding, which is useful in our attack strategy.

A. The three-party QKD protocols

In Ref. [24] two three-party QKD protocols were proposed. One deals with an honest center and the other is with an untrusted center. In the following description, for the sake of simplicity, we will call these two protocols QKDP-I and QKDP-II, respectively, and use the same notations as that in Ref. [24].

Now let us see QKDP-I first, where the technique of “block transmission”, proposed in Ref. [14], is utilized. This protocol is composed with the following steps (see Fig.1).

1. The center generates n qubits $|0\rangle$ and sends this sequence (denoted as Q_1) to Alice.

2. After receiving Q_1 , Alice selects a u -bit random session key K and computes its m -bit hash value $h = H(K)$ as the checksum, where $u + m = n$. Then Alice performs unitary operation $U_0 = I$ ($U_1 = i\sigma_y$) on the i -th qubit ($1 \leq i \leq n$) in Q_1 if the i -th bit in $K||h$ is 0 (1). Furthermore, Alice generates an n -bit random string B_1 , and performs unitary operation $U_0 = I$ ($U_2 = H$) on the i -th qubit in Q_1 if the i -th bit in B_1 is 0 (1). After these coding operations Alice sends the new qubit sequence (denoted as Q_2) to Bob. Here

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i\sigma_y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (1)$$

3. After receiving Q_2 , Bob selects two n -bit random strings R_2 and B_2 . Then he performs unitary operation U_0 or U_1 on each qubit in Q_2 according to R_2 , and then operation U_0 or U_2 on each qubit according to B_2 . These coding operations are similar to Alice’s in the previous step. Afterwards Bob sends the new qubit sequence (denoted as Q_3) to the center.

4. The center informs Alice and Bob after the receiving of Q_3 .

5. Alice and Bob tell the center B_1 and B_2 respectively.

6. According to $B_1 \oplus B_2$, the center recovers the original polarization bases of qubits by performing U_0 or U_2 on each qubit as in steps 2 and 3. Then the center measures all the qubits in basis $R = \{|0\rangle, |1\rangle\}$, obtaining the measurement results $C' = R_2 \oplus (K||h)$. At last the center announces C' to Bob.

7. Bob recovers $K||h = R_2 \oplus C'$ and verifies whether $h = H(K)$. If it is correct, Bob obtains the session key K and tells Alice it is successful.

This is the end of QKDP-I. In addition, Alice and Bob would also take some measures to prevent Trojan horse attack. In this protocol the operations of qubit generation and measurement are focused in the center’s lab, and Alice and Bob only need to perform unitary operations on the qubits. As analyzed in Ref. [24], this protocol has high efficiency.

It is easy to see that the center can obtain the session key in QKDP-I if he/she is not honest [24]. QKDP-II can resolve this problem, which is suitable for the situation where the center is untrusted. Now we introduce QKDP-II in brief (see Fig.2), which is useful when we discuss how to improve the protocols in section IV. The first two steps are the same as that in QKDP-I. After Bob received Q_2 , Alice tells Bob the value of B_1 . According to B_1 , Bob performs I or H to recover the original polarization bases of the qubits. Then Bob shuffles the sequence of qubits and sends it (denoted as Q_3) to the center. Here the shuffle operation is actually the technique of “order rearrangement” proposed in Ref. [44]. When the center receives Q_3 , he/she measures all qubits in basis R , and announces the results $C' = shuffled_K||h$ to Bob. At last Bob rearranges the string C' to obtain $K||h$, and checks whether $h = H(K)$. If it is correct, Bob tells Alice it is successful.

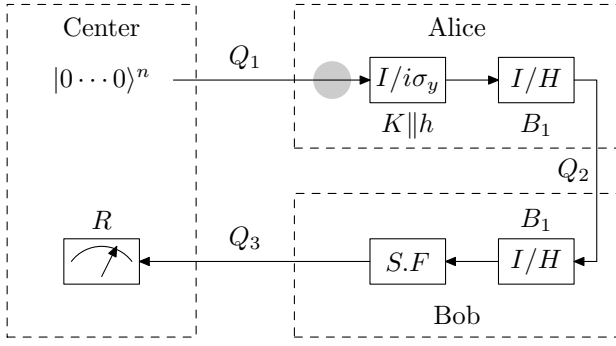


Fig. 2. The process of QKDP-II. The classical communications are omitted. $S.F$ denotes the shuffle operation, and the gray circle represents the position where another shuffle operation should be added to improve the protocol.

B. Dense coding

In 1992 C. H. Bennett and S. J. Wiesner presented a special feature of Einstein-Podolsky-Rosen (EPR) states, i.e. dense coding [43]. It was shown that two bits of classical information can be encoded into an EPR state by one-particle unitary operations. Specifically, if Alice and Bob hold one particle from an EPR state respectively, Alice can send two bits to Bob by performing one of four unitary operations on her particle and transmitting it to Bob. One particle carries two bits of information, which is the reason why it is called dense coding. Now we describe how it happens in brief.

Four EPR states are

$$\begin{aligned} |\Phi^\pm\rangle_{12} &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{12}, \\ |\Psi^\pm\rangle_{12} &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{12}, \end{aligned} \quad (2)$$

where the subscripts 1 and 2 denote different particles. These states are orthogonal with each other and compose a complete basis, i.e. Bell basis B_{Bell} . There are also four one-particle unitary operations I , σ_x , $i\sigma_y$, and σ_z , where

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (3)$$

Without loss of generality, suppose Alice and Bob share an EPR state $|\Phi^+\rangle_{12}$, that is, Alice has particle 1 and Bob holds 2. Alice can encode two bits of information into the state by performing one of the above four operations on particle 1, under which this state changes as

$$\begin{aligned} I^1|\Phi^+\rangle_{12} &= |\Phi^+\rangle_{12}, & \sigma_x^1|\Phi^+\rangle_{12} &= |\Psi^+\rangle_{12}, \\ (i\sigma_y)^1|\Phi^+\rangle_{12} &= |\Psi^-\rangle_{12}, & \sigma_z^1|\Phi^+\rangle_{12} &= |\Phi^-\rangle_{12}, \end{aligned} \quad (4)$$

where the superscript represents the qubit on which the operations are performed. Afterwards Alice sends particle 1 to Bob. Bob can distinguish which operation is chosen by Alice via a Bell measurement on particles 1 and 2. If I , σ_x , $i\sigma_y$, and σ_z represent 00, 01, 10, and 11 respectively, Bob can obtain two bits from Alice. For example, Bob knows Alice's message is 10 if his measurement result is $|\Psi^-\rangle_{12}$. Similarly, any one of the four EPR states can be used as the original state in this communication.

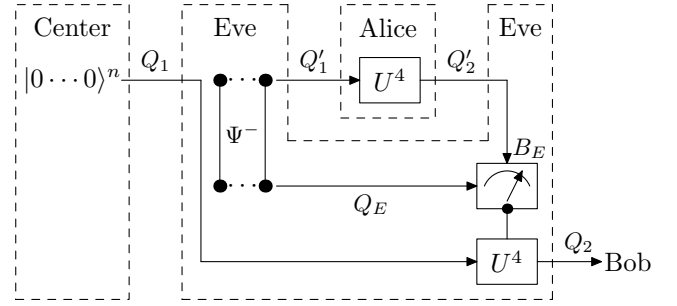


Fig. 3. Dense-coding attack on QKDP-I. The classical communications are omitted. U^4 represents one of the four operations $\{I, i\sigma_y, H, Hi\sigma_y\}$.

In fact, the above dense coding can be generalized to that using other entangled states and operations. In the following we will utilize this idea to design an effective attack on QKDP-I and QKDP-II, where Eve can totally obtain the transmitted key without being discovered.

III. DENSE-CODING ATTACK

We take QKDP-I as our example to analyze its security. In this protocol, Alice encodes the session key K into the qubits in Q_1 by unitary operations I and $i\sigma_y$. To prevent Eve from obtaining K from these qubits, Alice randomly changes the basis of each qubit by I and H . After the above two operations every qubit is randomly in one of four nonorthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then Alice sends the new sequence Q_2 to Bob. If Eve intercepts Q_2 and wants to obtain K by measurements, she cannot distinguish the above four states with certainty and disturbance will be inevitably introduced to the quantum states. This is very similar with that in BB84 QKD protocol [5].

However, as we know, fake-signal attack [41] is very common in the analysis of quantum cryptography. If Eve replaces the qubits in Q_1 by the ones from some entangled states, can she obtain K by collective measurements after Alice encoded and sent them out? This question is very interesting and difficult to give an answer. In fact, the answer is yes. This attack just like that Alice sends the secret key to Eve by an “unnoticed dense coding”. In the following we will depict this attack first and then prove its correctness.

Eve's dense-coding attack is as follows (see Fig.3).

E1. Eve generates n ordered EPR pairs in the state $|\Psi^-\rangle_{12}$. All the qubits with subscript 1 (2) compose a qubit sequence Q'_1 (Q_E).

E2. When the center sends the sequence Q_1 to Alice in Step 1, Eve intercepts all the qubits and replaces them by the sequence Q'_1 .

E3. When Alice sends the sequence Q'_2 , i.e. the qubits after Alice's encoding operations, to Bob in Step 2, Eve intercepts it and performs collective measurements on every pair of the corresponding qubits in Q'_2 and Q_E in the basis $B_E = \{|\Psi^-\rangle, |\Phi^+\rangle, |\Omega\rangle, |\Gamma\rangle\}$. Here

$$\begin{aligned} |\Omega\rangle_{12} &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)_{12}, \\ |\Gamma\rangle_{12} &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{12}, \end{aligned} \quad (5)$$

and it is easy to verify that $|\Psi^-\rangle$, $|\Phi^+\rangle$, $|\Omega\rangle$, and $|\Gamma\rangle$ are orthogonal with each other.

E4. Eve performs one of the four operations $\{I, i\sigma_y, H, Hi\sigma_y\}$ on every legal qubits in the sequence Q_1 according to her measurement result. In particular, Eve performs $I, i\sigma_y, H, Hi\sigma_y$ on the i -th qubit in Q_1 when her measurement result on the i -th pair is $|\Psi^-\rangle, |\Phi^+\rangle, |\Omega\rangle, |\Gamma\rangle$, respectively. Then Eve sends the new sequence Q_2 , i.e. the legal qubits after Eve's operations, to Bob.

E5. Eve obtains $K\|h$ from her measurement results in Step E3. That is, she knows the i -th bit of $K\|h$ is 0 (1) if her measurement result on the i -th pair is $|\Psi^-\rangle$ or $|\Omega\rangle$ ($|\Phi^+\rangle$ or $|\Gamma\rangle$).

By this strategy, Eve will obtain the key K correctly if we do not consider the errors brought by channel noise or other eavesdroppings. Furthermore, as we will show, this attack will not be discovered by legal users. Therefore, it is very effective though it looks quite simple.

Now we prove the correctness of our attack on QKDP-I. In fact, Alice's two encoding operations $I/i\sigma_y$ and I/H can be treated as one operation, i.e. one of $\{I, i\sigma_y, H, Hi\sigma_y\}$. If Eve can distinguish which one of the four operations is used by Alice in her encoding, Eve will obtain not only $K\|h$ but also B_1 . This situation is quite similar to that of dense coding. It is not difficult to verify that the four states in Eve's measurement basis B_E satisfies

$$\begin{aligned} |\Psi^-\rangle_{12} &= I^1 |\Psi^-\rangle_{12}, |\Phi^+\rangle_{12} = (i\sigma_y)^1 |\Psi^-\rangle_{12}, \\ |\Omega\rangle_{12} &= H^1 |\Psi^-\rangle_{12}, |\Gamma\rangle_{12} = (Hi\sigma_y)^1 |\Psi^-\rangle_{12}. \end{aligned} \quad (6)$$

Therefore, when Alice performs her encoding operations on the fake qubits in Q'_1 , the quantum state changes as described in Tab.1.

Tab.1. State changes after Alice's encoding on the fake qubits. The first and the last columns are the original and the final states of Eve's entangled pairs, respectively. The second and third columns are bit values of $K\|h$ and B_1 , respectively. The fourth column is the combined operation for Alice's encoding.

Orig. Stat.	$k\ h$	B_1	Comb. Oper.	Fina. Stat.
$ \Psi^-\rangle$	0	0	I	$ \Psi^-\rangle$
$ \Psi^-\rangle$	0	1	H	$ \Omega\rangle$
$ \Psi^-\rangle$	1	0	$i\sigma_y$	$ \Phi^+\rangle$
$ \Psi^-\rangle$	1	1	$Hi\sigma_y$	$ \Gamma\rangle$

Consider the i -th pair of qubits as our example, which is originally generated by Eve in the state $|\Psi^-\rangle_{12}$. When Eve sends the first qubit to Alice in Step E2, Alice will encode the i -th bits of $K\|h$ and B_1 on it. Without loss of generality, if the i -th bits of $K\|h$ and B_1 are 1 and 0 respectively, as shown in the fourth row in Tab.1, Alice's combined operation will be $i\sigma_y$, and then the state will be changed into $|\Phi^+\rangle$ after the encoding.

It can be seen from Tab.1 that four possible final states include $|\Psi^-\rangle$, $|\Phi^+\rangle$, $|\Omega\rangle$, and $|\Gamma\rangle$, which are orthogonal

with each other and can be distinguished with certainty by measurements in basis B_z . Therefore, Eve's measurement results $|\Psi^-\rangle$, $|\Phi^+\rangle$, $|\Omega\rangle$, and $|\Gamma\rangle$ on the i -th pair imply that the i -th bits of $K\|h$ and B_1 are 00, 10, 01, and 11, respectively. As a result, Eve can get the correct session key in Step E5.

Obviously, with the knowledge that which operations has been chosen by Alice, Eve just performs the same operations on the legal qubits in Q_1 in step E4. Therefore, the states of the new sequence Q_2 is the same as the situation where no eavesdropping happens. Consequently, no errors will be introduced by this attack and Eve will never be discovered. Note that every fake signal Eve sends to Alice only contains one ordinary qubit, which is different from a spy photon or invisible photon, and hence it would be unnoticed by Alice's apparatus, including that to prevent Trojan horse attack.

In a word, the dense-coding attack is correct and very effective for QKDP-I. Additionally, this attack is also suitable for QKDP-II because there is no difference between both protocols when Alice's encoding operations are considered (see Alice's areas in Fig.1 and Fig.2).

IV. DISCUSSIONS

Now we give some discussions about the security of two three-party QKDPs and our attack.

As we all know, fake-signal attack is very common in quantum cryptography and some effective manners to prevent it have been found. Then a question arises, i.e., why the three-party QKDPs are susceptible to such a familiar attack? In fact quite a few protocols [45], [46], [47] use similar properties of single photons, including the carrier states and the encoding operations, but they are all secure against this kind of attack. By careful comparison between the three-party QKDPs and these secure ones we can find the answer of the above question. That is, in the secure protocols the users will detect eavesdropping by some manners such as conjugate-basis measurements after he/she received the qubits, while it does not happen in the three-party QKDPs. Obviously, without any detections, Alice can never discover that the qubits were replaced by Eve when they were transmitted in public channel. In the three-party QKDPs, to reduce the cost of users, Alice and Bob have no measurement apparatus, and consequently cannot take general measures to detect eavesdropping. Though Bob checks whether $h = H(K)$ at last, which is the only detection in the three-party QKDPs, it is not strong enough. Therefore, it should be emphasized that more attention should be paid to the protocol's security when we pursue low expenses for the users because low expenses generally implies low capability to detect eavesdropping.

Now we discuss how to improve the three-party QKDPs to stand against the dense-coding attack. Note that in QKDP-II the operation of shuffle is utilized to prevent a dishonest center from obtaining the key. Actually this technique can also be used to protect the protocol against Eve's dense-coding attack. If Alice adds a shuffle operation before her encodings in QKDP-II (the position is denoted by the gray circle in Fig.2), Eve's attack will be of no effect. On the one hand, after Alice's encoding every qubit in Q'_2 is in the same state, i.e. the

maximally mixed state $\rho = I$, and then Eve cannot distinguish them and know which two qubits are originally in an entangled pair. Therefore, the measurement result will be random if Eve still measures every two qubits in the same position in Q'_2 and Q_E . Thus, Eve cannot distill the key from her measurement results and the eavesdropping will be discovered when Bob checks whether $h = H(K)$. On the other hand, because all qubits in Q_1 are in the same state $|0\rangle$, the additional shuffle brings no changes for legal qubits. As a result, this simple modification is very effective and interesting in the sense that it can prevent the dense-coding attack but has no effects to the protocol when no eavesdropping happens.

As shown above, the three-party QKDPs are insecure under the dense-coding attack. One may want to know what is wrong with the security proof in Ref. [24]. In fact the authors of Ref. [24] presented a formal proof with the sequence-of-games approach, which is often used in classical cryptography [48], [49], [50]. However, the attack strategies considered in this proof are not complete and the dense-coding attack is overlooked. As we know, quantum mechanics have many interesting or even counterfactual features. They not only give convenience for the users to distribute a secret key but also bring different kinds of new attack strategies for the eavesdropper. Therefore, more attention should be paid to all kinds of possible attacks in analyzing the security of a quantum cryptographic protocols.

V. CONCLUSION

Recently, two novel three-party QKDPs were proposed, in which, to save the expense, qubit generation and measurement are not needed for Alice and Bob [24]. In this paper we analyze the security of these protocols and find that they are susceptible to a special attack, i.e. the dense-coding attack. In this attack the eavesdropper Eve can obtain all the session key by sending entangled qubits to Alice and performing collective measurements after Alice's encoding, which is just like the process of dense coding between Eve and Alice. Furthermore, this attack does not introduce any errors to the transmitted information and consequently will not be discovered by Alice and Bob. The attack strategy is described in detail and a proof for its correctness is given. At last, a possible way to improve these protocols is discussed.

ACKNOWLEDGMENT

This work is supported by NSFC (Grant Nos. 60873191, 60903152, 61003286, 60821001), SRFDP (Grant Nos. 200800131016, 20090005110010), Beijing Nova Program (Grant No. 2008B51), Key Project of Chinese Ministry of Education (Grant No. 109014).

REFERENCES

- [1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in *Proc. 35th Annual Symposium on the Foundations of Computer Science*, Santa Fe, New Mexico, 1994, pp.124-134.
- [2] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proc. 28th Annual ACM Symposium on Theory of Computing*, New York, 1996, pp.212-219.
- [3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, vol.74, pp.145-195, 2002.
- [4] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, A. Tomita, "Practical quantum cryptosystem for metro area applications", *IEEE J. Sel. Top. Quant. Electron.*, vol.13, pp.1031-1038, 2007.
- [5] C. H. Bennett and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing", in *Proc. IEEE International Conference on Computers, Systems and Signal*, Bangalore, India, 1984, pp.175-179.
- [6] K. Inoue, "Quantum key distribution technologies", *IEEE J. Sel. Top. Quant. Electron.*, vol.12, pp.888-896, 2006.
- [7] A. Tanaka, W. Maeda, S. Takahashi, A. Tajima, A. Tomita, "Ensuring quality of shared keys through quantum key distribution for practical application", *IEEE J. Sel. Top. Quant. Electron.*, vol.15, pp.1622-1629, 2009.
- [8] H. P. Yuen, "Key generation: foundations and a new quantum approach", *IEEE J. Sel. Top. Quant. Electron.*, vol.15, pp.1630-1645, 2009.
- [9] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks", *IEEE J. Sel. Top. Quant. Electron.*, vol.16, pp.1591-1601, 2009.
- [10] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network", *Chinese Sci. Bull.*, vol.54, pp.2991-2997, 2009.
- [11] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret", *Phys. Rev. Lett.*, vol.83, pp.648-651, 1999.
- [12] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing", *Phys. Rev. A*, vol.59, pp.1829-1834, 1999.
- [13] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting", *Phys. Rev. A*, vol.59, pp.162-168, 1999.
- [14] G. Long and X. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme", *Phys. Rev. A*, vol.65, p.032302, 2002.
- [15] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement", *Phys. Rev. Lett.*, vol.89, p.187902, 2002.
- [16] F. Deng, G. Long, and X. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block", *Phys. Rev. A*, vol.68, p.042317, 2003.
- [17] W. Cao, Y. Yang, and Q. Wen, "Quantum secure direct communication with cluster states", *Sci. China Phys. Mech. Astron.*, vol.53, pp.1271-1275, 2010.
- [18] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel", *Sci. China Ser. G Phys. Mech. Astron.*, vol.52, pp.1208-1212, 2009.
- [19] M. Dusek, O. Haderka, M. Hendrych, and R. Myska, "Quantum identification system", *Phys. Rev. A*, vol.60, pp.149-156, 1999.
- [20] G. Zeng and W. Zhang, "Identity verification in quantum key distribution", *Phys. Rev. A*, vol.61, p.022303, 2000.
- [21] X. Zhang, "One-way quantum identity authentication based on public key", *Chinese Sci. Bull.*, vol.54, pp.2018-2021, 2009.
- [22] C. Li, H. Zhou, Y. Wang, and F. Deng, "Secure quantum key distribution network with Bell states and local unitary operations", *Chinese Phys. Lett.*, vol.22, pp.1049-1052, 2005.
- [23] S. Phoenix, S. Barnett, P. Townsend, and K. Blow, "Multi-user quantum cryptography on optical networks", *J. Modern Opt.*, vol.42, pp.1155-1163, 1995.
- [24] H. Shih, K. Lee, and T. Hwang, "New efficient three-party quantum key distribution protocols", *IEEE J. Sel. Top. Quant. Electron.*, vol.15, pp.1602-1606, 2009.
- [25] H. K. Lo and T. M. Ko, "Some attacks on quantum-based cryptographic protocols", *Quantum Inf. Comput.*, vol.5, pp.41-48, 2005.
- [26] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Comment on 'Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection'", *Phys. Rev. Lett.*, vol.101, p.208901, 2008.
- [27] Y. Zhang, C. Li, and G. Guo, "Comment on 'Quantum key distribution without alternative measurements'", *Phys. Rev. A*, vol.63, p.036301, 2001.
- [28] F. Gao, Q. Wen, and F. Zhu, "Teleportation attack on the QSDC protocol with a random basis and order", *Chinese Phys. B*, vol.17, pp.3189-3193, 2008.
- [29] G. Gao, "Reexamining the security of the improved quantum secret sharing scheme", *Opt. Commun.*, vol.282, pp.4464-4466, 2009.
- [30] Z. Zhu and Y. Zhang, "Cryptanalysis and Improvement of a Quantum Secret Sharing Protocol between Multiparty and Multiparty with Single Photons and Unitary Transformations", *Chin. Phys. Lett.*, vol.27, p.060303, 2010.
- [31] A. Wójcik, "Eavesdropping on the 'ping-pong' quantum communication protocol", *Phys. Rev. Lett.*, vol.90, p.157901, 2003.
- [32] A. Wójcik, "Comment on 'Quantum dense key distribution'", *Phys. Rev. A*, vol.71, p.016301, 2005.

- [33] Q. Cai, "The 'Ping-Pong' protocol can be attacked without eavesdropping", *Phys. Rev. Lett.*, vol.91, p.109801, 2003.
- [34] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Consistency of shared reference frames should be reexamined", *Phys. Rev. A*, vol.77, p.014302, 2008.
- [35] F. Gao, Q. Y. Wen, and F. C. Zhu, "Comment on: 'Quantum exam' [Phys. Lett. A 350 (2006) 174]", *Phys. Lett. A*, vol.360, pp.748-750, 2007.
- [36] F. Gao, S. Lin, Q. Y. Wen, and F. Zhu, "A special eavesdropping on one-sender versus N-receiver QSDC protocol", *Chinese Phys. Lett.*, vol.25, pp.1561-1563, 2008.
- [37] F. Gao, S. Qin, Q. Wen, and F. Zhu, "Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state", *Opt. Commun.*, vol.283, pp.192-195, 2010.
- [38] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantumkey-Distribution systems," *Phys. Rev. A*, vol.73, p.022320, 2006.
- [39] F. Deng, X. Li, H. Zhou, and Z. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack", *Phys. Rev. A*, vol.72, p.044302, 2005.
- [40] F. Gao, S. Qin, Q. Wen, and F. Zhu, "A simple participant attack on the Bradler-Dusek protocol", *Quantum Inf. Comput.*, vol.7, pp.329-334, 2007.
- [41] S. Qin, F. Gao, Q. Wen, and F. Zhu, "Improving the security of multiparty quantum secret sharing against an attack with a fake signal", *Phys. Lett. A*, vol.357, pp.101-103, 2006.
- [42] L. Hao, J. Li, and G. LONG, "Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution", *Sci. China Phys. Mech. Astron.*, vol.53, pp.491-495, 2010.
- [43] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states", *Phys. Rev. Lett.*, vol.69, pp.2881-2884, 1992.
- [44] F. Deng and G. Long, "Controlled order rearrangement encryption for quantum key distribution", *Phys. Rev. A*, vol.68, p.042315, 2003.
- [45] F. Deng and G. Long, "Secure direct communication with a quantum one-time pad", *Phys. Rev. A*, vol.69, p.052319, 2004.
- [46] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement", *Phys. Rev. Lett.*, vol.94, p.140501, 2005.
- [47] F. Deng, H. Zhou, and G. Long, "Bidirectional quantum secret sharing and secret splitting with polarized single photons", *Phys. Lett. A*, vol.337, pp.329-334, 2005.
- [48] V. Shoup. (2006). Sequences of games: A tool for taming complexity in security proof, Cryptology ePrint Archive, Rep. 2004/332 [Online]. Available: <http://www.shoup.net/>
- [49] D. Nowak, "A framework for game-based security proofs", *Inf. Commun. Security*, vol.4861, pp.319-333, 2007.
- [50] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption", *J. Cryptol.*, vol.20, pp.203-235, 2007.